معرفی سامانه کنترل دسترسی به شبکه

پادویش - Padvish NAC

شرکت نرم افزاری امن پرداز

سطح محرمانگی: عادی

نسخه ۱.۰

زمستان ۱۴۰۴

فهرست مطالب

مقدمه – ضرورت کنترل دسترسی هوشمند شبکه

در چشم انداز تهدیدات سایبری دسترسی کنترل‌نشده به شبکه یکی از مهم‌ترین نقاط ضعف امنیتی سازمان‌ها است. در این چشم انداز محیط شبکه سنتی فضایی را ایجاد نموده که در آن، شبکه داخلی دیگر نمی‌تواند به طور پیش‌فرض قابل اعتماد باشد. این واقعیت چندین چالش عملیاتی متمایز و حیاتی را ایجاد نموده که منجر به تضعیف وضعیت امنیتی سازمان ها شده است.

اولین چالش: اتصال دستگاه‌ها به شبکه بدون احراز هویت امنیتی قبلی است، جایی که در آن نقاط پایانی شبکه صرفاً بر اساس امکان اتصال به پورت شبکه یا نقطه دسترسی بی‌سیم، بدون هیچ گونه تأییدی مجوز دسترسی می‌گیرند. این موضوع فرصتی برای اتصال دستگاه‌های محافظت نشده یا غیرمنطبق با سیاست امنیتی سازمان را ایجاد می‌کند و زمینه ساز مشکلات جزئی‌تر مانند امکان دسترسی غیرمجاز از طریق نصب یک سیستم‌عامل ثانویه و دور زدن سیاست‌ها یا تهدیدات ناشی از Live OS که کنترل‌های نرم‌افزاری امنیتی را کاملاً دور می‌زند، می‌باشد.

چالش دوم: اجرای دستی و پراکنده سیاست‌های امنیتی در سازمان است. در بسیاری از سازمان‌ها سیاست های امنیتی وجود داشته اما به طور خودکار توسط زیرساخت شبکه اجرا نمی‌شوند. مدیران شبکه مجبورند کنترل‌ها را به صورت دستی در سیستم‌های مختلف اجرا کنند – پیکربندی تنظیمات پورت سوئیچ، به‌روزرسانی قوانین فایروال و تنظیم سیاست‌های شبکه به صورت جزیره‌ای. این رویکرد نه تنها کند و پرزحمت است، بلکه بسیار مستعد خطای انسانی است که شکاف‌های امنیتی ایجاد می‌کند.

چالش مهم سوم: فرآیند وقت‌گیر لغو دسترسی در صورت لزوم یا تغییر در شرایط امنیتی دستگاه نقاط پایانی است. هنگامی که دستگاهی مشکوک به رخنه امنیتی است یا به عنوان دستگاهی غیر منطبق با سیاست های امنیتی سازمان شناسایی می‌شود، فرآیند جداسازی آن از شبکه اغلب نیاز به مداخله دستی در چندین سیستم دارد، که در این مدت دستگاه می‌تواند به ایجاد تهدید ادامه دهد و به طور بالقوه حرکت جانبی را برای یک مهاجم تسهیل کند.

Padvish NAC پاسخی هوشمندانه به این چالش‌ها است. این راهکار به مدیران شبکه توانایی می‌دهد تا از وضعیت امنیتی واکنشی به وضعیت پیشگیری فعال حرکت کنند. این راهکار نشان‌دهنده تغییر اساسی از اعتماد

به همه دستگاه‌های داخل شبکه به مدلی از تأیید و اجرای مستمر است. این راهکار طراحی شده است تا تضمین کند که هر دستگاه و کاربری که به شبکه متصل می‌شود، قبل از اعطای دسترسی، با سیاست‌های امنیتی سازمان مطابقت دارد.

این محصول با انجام تأیید بلادرنگ وضعیت نصب بودن آنتی‌ویروس، سطح وصله‌ها، یکپارچگی سیستم عامل و احراز هویت کاربر، به طور پویا سیاست‌های دسترسی را برای حفظ انطباق و امنیت مستمر اجرا می‌کند. این تأیید بلادرنگ در لحظه اتصال رخ می‌دهد و در طول نشست دستگاه ادامه می‌یابد و تضمین می‌کند که هر تغییر در وضعیت انطباق بلافاصله رسیدگی می‌شود.

این محصول ابزارهای لازم برای حفظ دید، کنترل و اعتماد در هر نقطه اتصال را برای سازمان ها فراهم می‌کند.

این سیستم بر اساس سیاست سختگیرانه «دسترسی به شبکه فقط در صورت محافظت شدن دستگاه» عمل می‌کند که هسته فلسفه امنیتی آن را تشکیل می‌دهد. این سیاست به این معنی است که دسترسی به منابع شبکه فقط به پایانه‌های تأیید شده و مطابق که نشان داده‌اند الزامات امنیتی سازمان را برآورده می‌کنند، اعطا می‌شود. این رویکرد با تأیید وضعیت محافظت هر دستگاه در زمان دسترسی، تهدیدات را قبل از ورود به شبکه متوقف می‌کند و کاهش خطر فوری را ارائه می‌دهد.

۱. نمای کلی معماری

Padvish NAC یک راهکار یکپارچه برای **کنترل، نظارت و خودکارسازی دسترسی به شبکه** است. این سیستم اقدامات کنترلی پراکنده را با یک چارچوب متمرکز و مبتنی بر سیاست های امنیتی از پیش تعریف شده توسط سازمان، جایگزین می‌کند. این راهکار با همکاری با سرور مدیریتی پادویش (PMS) به صورت هوشمند سیاست‌های امنیتی سازمان را اجرا می‌کند. این یکپارچگی به Padvish NAC امکان می‌دهد از داده‌های امنیتی غنی جمع‌آوری‌شده توسط اکوسیستم پادویش برای ارزیابی وضعیت امنیتی هر دستگاه استفاده کند.

این محصول حول سه مؤلفه اصلی طراحی شده است که با همکاری هم **یک راهکار جامع کنترل دسترسی شبکه** ارائه می‌دهند.

۱/۱/۱. هسته (موتور تصمیم‌گیری)

این راهکار در هسته مرکزی خود دارای یک موتور تصمیم گیری است که مسئول پردازش قوانین امنیتی و مدیریت تصمیمات دسترسی است. در این موتور تصمیم گیری داده‌های جمع‌آوری‌شده از سنسورها پردازش شده و سطح دسترسی مناسب هر دستگاه بر اساس سیاست‌های از پیش تعیین شده تعیین می‌شود. هسته تمام شرایط و معیارهای تعریف‌شده در سیاست‌های سازمان را ارزیابی و حکم نهایی دسترسی را صادر می‌کند. همچنین، هسته نقطه مرکزی پیکربندی و مدیریت سیستم و میزبان رابط مدیریتی است که در آن سیاست‌ها تعریف و وضعیت کل سیستم نظارت می‌شود.

۱/۱/۲. سنسورها (جمع‌آوری داده)

این مؤلفه‌ها داده‌ها را از پایانه‌های تعیین شده و سرور مدیریتی پادویش جمع‌آوری می‌کنند و به عنوان منبع حقیقت وضعیت واقعی دستگاه‌ها عمل می‌کنند. سنسورها شامل اطلاعاتی از وضعیت آنتی‌ویروس، پیکربندی فایروال، نسخه سیستم عامل، سطح وصله‌ها و نتایج اسکن آسیب‌پذیری هستند. جمع‌آوری بلادرنگ داده‌ها تضمین می‌کند که تصمیمات کنترل دسترسی بر اساس اطلاعات دقیق و به‌روز گرفته می‌شوند.

۱/۱/۳. عملگرها (عامل اجرا)

عملگرها تصمیمات NAC را مستقیماً در زیرساخت شبکه اعمال می‌کنند. آن‌ها دستورات هسته را به اقدامات مشخص شبکه ترجمه می‌کنند، مانند اجازه یا مسدود کردن ترافیک، و در نقاط کلیدی شبکه مستقر می‌شوند. عملگرها دستورات هسته را دریافت و با استفاده از مکانیزم‌های اجرایی تصمیمات سیاستی را پیاده‌سازی می‌کنند.

۲. ویژگی‌ها و قابلیت‌های محصول

۲/۱. داشبورد اصلی

داشبورد به عنوان مرکز اصلی برای نظارت بر سیستم عمل می‌کند. این رابط نمای جامعی از وضعیت شبکه، از جمله کلاینت‌ها، سرورها و عملگرها ارائه می‌دهد و به مدیران یک نمای واحد برای مدیریت امنیت دسترسی شبکه می‌دهد.

- **عملکرد:** داشبورد تعداد و وضعیت تمام کلاینت‌ها، سرورها و عملگرهای Padvish NAC را نمایش می‌دهد. این اطلاعات را با استفاده از نمودارهای زنده با شاخص‌های وضعیت کدگذاری شده رنگی (سالم، هشدار، خطا) ارائه می‌دهد و به مدیران امکان می‌دهد به سرعت سلامت کلی استقرار این راهکار را ارزیابی کرده و مناطق نیازمند توجه را در یک نگاه شناسایی کنند.
- **بینش عملیاتی:** این داشبورد یک گزارش بلادرنگ از دستگاه‌هایی که Padvish NAC روی آنها فعال یا غیرفعال است ارائه می‌دهد. مدیران می‌توانند وضعیت سلامت خلاصه مؤلفه‌های اصلی سیستم، از جمله سنسورها، قوانین و عملگرها را مشاهده کنند. این دید جامع امکان شناسایی فوری شکاف‌های پوشش که در آن حفاظت Padvish NAC ممکن است وجود نداشته باشد و همچنین مؤلفه‌هایی که ممکن است مشکل داشته باشند یا خارج از پارامترهای مورد انتظار عمل کنند را فراهم می‌کند.
- **به‌روزرسانی‌های پویا:** اطلاعات روی داشبورد به طور خودکار به‌روز می‌شود و تضمین می‌کند که مدیران همیشه دید فعلی از وضعیت امنیتی شبکه دارند.

۲/۲. بخش مدیریت سامانه

این بخش مسئول نظارت و هماهنگی تعامل بین سیستم Padvish NAC و سرورهای مدیریتی پادویش Padvish Management Server است.

- **یکپارچه‌سازی:** این بخش به مدیران اجازه می‌دهد سرورهای PMS را اضافه کنند، که منبع جمع‌آوری داده از نقاط پایانی هستند. فرآیند اضافه کردن یک سرور شامل مشخص کردن پارامترهای

اتصال از جمله نام، آدرس سرور و پورت سرور است. چندین سرور PMS را می‌توان برای تطبیق با استقرارهای توزیع شده یا ساختارهای مدیریت سلسله مراتبی اضافه کرد.

- **نظارت:** رابط وضعیت آخرین ارتباط با هر سرور، از جمله زمان آخرین اتصال و فاصله زمانی تا بررسی برنامه‌ریزی شده بعدی را نمایش می‌دهد. این دید برای تضمین یکپارچگی جریان داده بسیار مهم است، زیرا هر گونه وقفه در ارتباط با سرورهای PMS منجر به اطلاعات پایانه قدیمی یا مفقود شده می‌شود که به طور بالقوه می‌تواند به تصمیمات کنترل دسترسی نادرست منجر شود.
- **مدیریت:** این بخش قابلیت مشاهده و مدیریت همزمان چندین سرور را فراهم می‌کند. مدیران می‌توانند کنترل کنند که آیا هر سرور در چارچوب NAC فعال یا غیرفعال است، که اجازه حذف موقت سرورهای در حال تعمیر و نگهداری بدون حذف کامل آنها از پیکربندی را می‌دهد.

۲/۳. تعریف مجموعه قوانین

مجموعه قوانین (Ruleset) هسته منطق تصمیم‌گیری محصول Padvish NAC را تشکیل می‌دهند و تعریف و اجرای قوانین دسترسی شبکه را ممکن می‌سازند. آنها نشان‌دهنده کدگذاری سیاست‌های امنیتی سازمان به کنترل‌های فنی قابل اجرا هستند که سیستم Padvish NAC می‌تواند به طور خودکار در سراسر شبکه اعمال کند.

- **دسته‌بندی قوانین:** قوانین در پنج دسته اولیه برای ایجاد سیاست ساختاریافته سازماندهی شده‌اند:
  - **وضعیت کلاینت:** در این قسمت میتوان وضعیت کلاینت ها را بر اساس سیاست های گوناگون تعیین کرد. از جمله تعیین نام سرور، اطلاعات عمومی و وضعیت ارتباط دستگاه با سرور PMS را بررسی می‌کند. این شامل تأیید اینکه آیا دستگاه در حال حاضر آنلاین است و به درستی ارتباط برقرار می‌کند، بررسی گروه یا دامنه اختصاص داده شده، بررسی زمان آخرین ارتباط و تأیید زمان آخرین به‌روزرسانی پایگاه داده امنیتی می‌شود.
  - **ماژول‌های محافظ:** وضعیت مؤلفه‌های امنیتی، از جمله فایروال، محافظت بلادرنگ، محافظت در برابر دستکاری و ویژگی‌های محافظت از خود را تأیید می‌کند. این دسته تضمین می‌کند که تمام مکانیزم‌های امنیتی حیاتی فعال و مطابق با سیاست در حال عملکرد هستند.

- **آسیب‌پذیری:** سطح ریسک را بر اساس تعداد آسیب‌پذیری‌ها و زمان آخرین اسکن امنیتی ارزیابی می‌کند. این شامل شمارش کل آسیب‌پذیری‌ها، شناسایی CVE های بحرانی و ارزیابی این نکته میشود که آیا دستگاه اخیراً اسکن شده است؛ تا از به‌روز بودن داده آسیب‌پذیری اطمینان حاصل شود.
- **شبکه:** ویژگی‌های اتصال مانند آدرس MAC ، Gateway و دامنه شبکه را بررسی می‌کند. این امر امکان سیاست‌های مبتنی بر مکان شبکه، هویت دستگاه از طریق آدرس MAC و پارامترهای اتصال برای اجرای تقسیم‌بندی و محدودیت‌های دسترسی را فراهم می‌کند.
- **اطلاعات:** سیستم عامل، نسخه نرم‌افزار و سخت‌افزار دستگاه را شناسایی می‌کند. این امر سیاست‌هایی را ممکن می‌سازد که دسترسی را بر اساس نسخه‌های خاص سیستم عامل، انواع سخت‌افزار یا طبقه‌بندی‌های دستگاه مانند ایستگاه‌های کاری در مقابل سرورها محدود می‌کنند.

- **قابلیت‌های کلیدی:**
  - مدیران می‌توانند مجموعه قوانین کامل را تعریف، ویرایش و حذف کنند و مدیریت چرخه عمر کامل را برای سیاست‌های کنترل دسترسی فراهم می‌کنند.
  - برای هر شرط در یک قانون، نوع عملگر را می‌توان مشخص کرد (مانند مساوی، نامساوی، شامل، بزرگتر از، کوچکتر از)، که عبارات منطقی دقیق برای ارزیابی سیاست را ممکن می‌سازد.
  - چندین شرط را می‌توان در یک مجموعه قوانین واحد ترکیب کرد تا گزاره‌های منطقی پیچیده‌ای ایجاد کند که به طور دقیق نیازهای امنیتی پیچیده را منعکس کنند.
  - هر Rule را می‌توان به طور مستقل فعال یا غیرفعال کرد و امکان تنظیمات موقت سیاست بدون حذف و ایجاد مجدد قوانین را فراهم می‌کند.
  - قوانین را می‌توان ذخیره، ویرایش و در سیاست‌های کلی ترکیب کرد که می‌توانند در بخش‌های مختلف شبکه یا گروه‌های کاربری اعمال شوند.

- یک جدول مدیریتی وضعیت خلاصه تمام قوانین را ارائه می‌دهد و نمای سریعی از اینکه کدام قوانین فعال و پیکربندی پایه آنها چیست، ارائه می‌کند.
- سیستم از عملکرد همزمان چندین Ruleset پشتیبانی می‌کند و سیاست‌های مختلف برای بخش‌های مختلف شبکه یا انواع مختلف دستگاه‌ها را ممکن می‌سازد.

۲/۴. عملگرها

عملگرها مؤلفه‌های اجرایی سیستم Padvish NAC هستند که تصمیمات آن را مستقیماً در شبکه اعمال می‌کنند. آنها به عنوان پل بین تصمیمات سیاستی گرفته شده توسط هسته و زیرساخت شبکه واقعی که جریان ترافیک را کنترل می‌کند، عمل می‌کنند. در حال حاضر عملگرهایی همچون IP Set, Feed و Send to Url مورد استفاده قرار می‌گیرند.

- **نقش:** آنها مسئول پیاده‌سازی تصمیمات کنترل دسترسی گرفته شده توسط هسته هستند. هنگامی که هسته تعیین می‌کند که یک دستگاه باید دسترسی داشته باشد، مسدود شود یا در یک بخش شبکه محدود قرار گیرد، این عملگر است که این تصمیم را در محیط شبکه اجرا می‌کند.
- **مدیریت:** عملگرهای جدید را می‌توان از طریق کنسول در شبکه اضافه و مدیریت کرد. فرآیند شامل استقرار عملگر در مکان‌های شبکه مناسب و سپس ثبت آنها با هسته Padvish NAC است تا بتوانند دستورالعمل‌های اجرایی دریافت کنند.
- **نظارت:** زمان آخرین فعالیت و وضعیت ارتباط هر عملگر در رابط مدیریتی قابل مشاهده است. این به مدیران امکان می‌دهد تأیید کنند که تمام عملگرها عملیاتی هستند و به درستی با هسته ارتباط برقرار می‌کنند و اجرای یکنواخت سیاست در تمام بخش‌های شبکه را تضمین می‌کند.
- **تعیین سیاست:** سیاست‌ها و قوانین خاص را می‌توان به عملگرهای مجزا اختصاص داد. این امر اجرای هدفمند را ممکن می‌سازد جایی که بخش‌های مختلف شبکه می‌توانند سیاست‌های کنترل دسترسی مختلفی اعمال شده بر اساس الزامات امنیتی هر بخش داشته باشند.

- **بازخورد اجرا:** رابط وضعیت اجرای سیاست را نمایش می‌دهد. این مکانیزم بازخورد تأیید ارائه می‌دهد که دستورات اجرا با موفقیت توسط عملگرها دریافت و پیاده‌سازی شده‌اند و سیستم کنترل حلقه بسته را تکمیل می‌کند.

۲/۵. بخش تشخیص و بررسی

این صفحه برای شناسایی و حل خطاهای احتمالی در سیاست‌ها یا دستگاه‌ها استفاده می‌شود. این صفحه به عنوان رابط عیب‌یابی اولیه برای اپراتورهای امنیتی و مدیران شبکه عمل می‌کند و بینش‌های دقیقی در مورد عملیات و تصمیمات سیستم Padvish NAC ارائه می‌دهد.

- **نمای کلی کلاینت:** یک لیست کامل از تمام کلاینت‌ها به همراه وضعیت اتصال Padvish NAC آنها نمایش می‌دهد. این فهرست جامع هر دستگاهی که سیستم Padvish NAC از آن آگاه است را به همراه وضعیت دسترسی فعلی آن نشان می‌دهد و تصویر کاملی از تمام پایانه‌های شبکه ارائه می‌دهد.

- **بررسی انطباق:** وضعیت انطباق هر دستگاه در برابر سیاست‌های تعریف شده ارزیابی می‌شود. برای هر دستگاه، سیستم نشان می‌دهد که آیا در حال حاضر با تمام سیاست‌های قابل اعمال مطابقت دارد یا کدام سیاست‌های خاص را نقض می‌کند و تلاش‌های اصلاحی هدفمند را ممکن می‌سازد.

- **نمای جزئیات:** جزئیات کامل برای هر دستگاه در دسترس است، از جمله آدرس IP، عملگر مسئول، وضعیت دسترسی و زمان آخرین بررسی. این اطلاعات برای بررسی حوادث خاص یا درک اینکه چرا یک دستگاه خاص اجازه دسترسی پیدا کرده یا رد شده است، ضروری است.

- **عیب‌یابی:** ابزارهای تشخیصی سریع برای شناسایی علت اصلی نقض سیاست‌ها ارائه شده است. این ابزارها به مدیران کمک می‌کنند به سرعت تعیین کنند چرا یک دستگاه غیرمطابق است، مانند اینکه کدام شرط خاص در یک مجموعه قوانین شکست خورده است، و فرآیند حل را تسریع می‌کنند.

- **گزارش‌دهی:** گزارش‌گیری جامع در مورد عملکرد کلی سیستم Padvish NAC در سراسر شبکه در دسترس است. این گزارش‌ها می‌توانند روندهای انطباق، نقض سیاست‌ها و الگوهای دسترسی را نشان دهند و از تصمیم‌گیری عملیاتی و ارزیابی وضعیت امنیتی پشتیبانی می‌کنند.

۲/۶. کاربران و تنظیمات

این بخش مدیریت دسترسی کاربر و پیکربندی کلی سیستم را مدیریت می‌کند. این بخش دسترسی مدیریتی به سیستم NAC را کنترل می‌کند و پارامترهایی که بر عملکرد کلی سیستم تأثیر می‌گذارند را پیکربندی می‌کند.

- **مدیریت کاربر:** مدیران می‌توانند کاربران سیستم را اضافه، ویرایش یا حذف کنند. این شامل تعریف اطلاعات حساب پایه و اعتبارنامه‌های احراز هویت برای افرادی است که نیاز به دسترسی به رابط مدیریت Padvish NAC دارند.
- **کنترل دسترسی مبتنی بر نقش:** کاربران میتوانند با نقش های مشخص شده در شبکه سازمان قرار بگیرند. این امر اصل حداقل اختیار را با اطمینان از اینکه کاربران فقط به عملکردهای لازم برای مسئولیت‌های خود دسترسی دارند، ممکن می‌سازد.
- **دسترسی همزمان:** سیستم از چندین حساب مدیریتی همزمان پشتیبانی می‌کند. این امر اجازه می‌دهد مدیران مختلف به طور همزمان با سیستم بدون تعارض کار کنند و از عملیات امنیتی مبتنی بر تیم و کار شیفتی در سازمان‌های بزرگتر پشتیبانی می‌کند.
- **پیکربندی سیستم:** تنظیمات عمومی سیستم در اینجا مدیریت می‌شود، از جمله اطلاعات نسخه، تنظیمات به‌روزرسانی و پارامترهای عملکردی.

۳. قابلیت‌های عمومی و زیرساختی

این محصول با چندین قابلیت بنیادی ساخته شده است که از عملکرد آن در محیط‌های سازمانی پشتیبانی می‌کنند. این ویژگی‌های زیربنایی تضمین می‌کنند که راهکار برای استقرار، مدیریت و نگهداری در محیط‌های شبکه واقعی عملی است.

- **رابط وب:** یک رابط کاربرپسند مبتنی بر وب طراحی شده برای مدیران شبکه. این دسترسی مبتنی بر مرورگر به این معنی است که مدیران می‌توانند سیستم را از هر مکان بدون نیاز به نرم‌افزار کلاینت تخصصی مدیریت کنند، مدیریت را ساده کرده و قابلیت‌های مدیریت از راه دور را ممکن می‌سازند.

- **یکپارچه‌سازی با سرور مدیریتی پادویش**: هماهنگی کامل با سامانه مدیریت Padvish (PMS) یکی از قابلیت‌های اصلی این محصول است. این یکپارچه‌سازی به این معنی است که سیستم Padvish NACمی‌تواند از داده‌های امنیتی غنی پایانه که قبلاً توسط اکوسیستم Padvish جمع‌آوری شده است استفاده کند بدون اینکه نیاز به تلاش‌های جمع‌آوری داده تکراری یا پروژه‌های یکپارچه‌سازی پیچیده داشته باشد.
- **ثبت رویداد:** سیستم قابلیت‌های ثبت رویداد و گزارش‌دهی را از طریق ویژگی‌های تشخیص و ثبت رویداد ارائه می‌دهد.
- **طراحی سازمانی:** این راهکار با طراحی سبک، به صورت ماژولار و مقیاس‌پذیر برای محیط‌های سازمانی طراحی شده است.

۴. مزایای کلیدی برای سازمان‌ها و نهادها

Padvish NAC مزایای استراتژیک قابل توجهی ارائه می‌دهد و قابلیت‌های فنی را به نتایج عملی و ملموس سازمانی تبدیل می‌کند. این مزایا هم بر اثرگذاری امنیتی و هم بر بهبود کارایی عملیاتی تمرکز دارند و ارزشی فراتر از کنترل دسترسی پایه ارائه می‌کنند.

۴/۱. کنترل متمرکز دسترسی شبکه

تمام دستگاه‌ها بر اساس سیاست‌های امنیتی متمرکز سازمان ارزیابی می‌شوند. این رویکرد، اجرای یکنواخت سیاست‌ها را بدون توجه به محل یا نحوه اتصال دستگاه‌ها تضمین می‌کند و شکاف‌های امنیتی ناشی از اجرای پراکنده را از بین می‌برد.

نتیجه برای سازمان: حذف نقاط ورود ناشناخته. با اطمینان از اینکه هر دستگاه قبل از اعطای دسترسی با استانداردهای امنیتی یکسان بررسی می‌شود، سازمان‌ها می‌توانند نقاط دسترسی بدون محافظت را که مهاجمان ممکن است از آن‌ها سوءاستفاده کنند، حذف کنند.

۴/۲. عیب‌یابی سریع و شفاف

ماژول تشخیص سیستم به‌طور دقیق خطاها و نقض سیاست‌ها را شناسایی می‌کند. وقتی مشکلات دسترسی رخ می‌دهد، مدیران می‌توانند به سرعت علت آن را تعیین کنند، بدون اینکه درگیر فرآیند وقت‌گیر عیب‌یابی شبکه شوند. سیستم به وضوح نشان می‌دهد کدام شرط سیاست برآورده نشده است.

نتیجه برای سازمان :کاهش زمان حل مشکل. دید شفاف به علت مسائل دسترسی به مدیران امکان می‌دهد مشکلات را سریع حل کنند، تأثیر بر بهره‌وری را به حداقل برسانند و بار عملیاتی تیم‌های پشتیبانی را کاهش دهند.

۴/۳. یکپارچه‌سازی با PMS

داده‌های سرور مدیریتی پادویش مستقیماً در تصمیم‌گیری Padvish NAC استفاده می‌شوند و یک سیستم امنیتی حلقه بسته ایجاد می‌کنند. در این سیستم، وضعیت محافظت پایانه مستقیماً بر امتیاز دسترسی شبکه تأثیر دارد و اطمینان حاصل می‌کند که تصمیمات Padvish NAC بر اساس اطلاعات امنیتی جامع اتخاذ می‌شوند.

نتیجه برای سازمان: دید جامع از وضعیت امنیتی. همبستگی داده‌های امنیتی پایانه با کنترل دسترسی شبکه، نمای یکپارچه‌ای از وضعیت امنیتی فراهم می‌کند و مدیریت امنیتی مؤثرتر را ممکن می‌سازد.

۴/۴. نصب سریع و کم‌هزینه

استقرار مبتنی بر کانتینر نیازی به سخت‌افزار اختصاصی ندارد و امکان راه‌اندازی روی سرور استاندارد یا محیط‌های مجازی‌شده را فراهم می‌کند.

نتیجه برای سازمان :کاهش زمان و هزینه پیاده‌سازی. مدل استقرار ساده‌شده امکان اجرای سریع‌تر کنترل دسترسی شبکه را با سرمایه‌گذاری اولیه کمتر فراهم می‌کند و Padvish NAC در سطح سازمانی را برای طیف وسیعی از سازمان‌ها در دسترس قرار می‌دهد.

۴/۵. امن و قابل اطمینان

سیستم بدون وابستگی به سرویس‌های خارجی عمل می‌کند و هیچ داده پنهان یا غیرشفافی جمع‌آوری نمی‌کند، کنترل کامل بر داده‌های امنیتی را تضمین می‌کند.

نتیجه برای سازمان :انطباق با الزامات امنیت سایبری در سطح ملی. با عملکرد مستقل و مدیریت شفاف داده، این راهکار به سازمان‌ها کمک می‌کند تا با الزامات قانونی مطابقت داشته باشند.

۵. جمع بندی

Padvish NAC یک راهکار بومی و هوشمند برای کنترل و نظارت بر دسترسی در شبکه‌های سازمانی است. این سیستم نشان‌دهنده یک تغییر اساسی در رویکرد سازمان‌ها به امنیت شبکه است و از مدل اعتماد ضمنی به دستگاه‌ها، به **تأیید مستمر و کنترل دسترسی مبتنی بر سیاست** حرکت می‌کند.

با جمع‌آوری داده‌های واقعی از کلاینت‌ها – شامل وضعیت محافظتی، آسیب‌پذیری‌ها و شرایط شبکه – به مدیران امکان می‌دهد قوانین دقیق و خودکار برای ورود و خروج دستگاه‌ها تعریف کنند. به جای واکنش تأخیری به تهدیدات، **Padvish NAC به طور پیشگیرانه عمل می‌کند**؛ هر دستگاه قبل از اعطای دسترسی ارزیابی می‌شود و تنها در صورت تطابق کامل با سیاست‌های امنیتی مجاز به اتصال است. این ارزیابی پیش از پذیرش، از دسترسی دستگاه‌های در معرض خطر یا غیرمطابق به منابع شبکه جلوگیری می‌کند و تهدیدات را در مرز متوقف می‌سازد. نتیجه، شبکه‌ای است که در آن **نظم، سلامت و اطمینان جایگزین ریسک و حدس‌وگمان می‌شود** و مدیران می‌توانند مطمئن باشند که هر دستگاه با استانداردهای امنیتی سازمان مطابقت دارد.